JC10 Rec'd PCT/PTO 2 8 SEP 2001

FORM PTO-1390 (REV. 11-2000) U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY 'S DOCKET NUMBER: M/ME/00v888US

U.S. APPLICATION NO (If known, see 37 CFR 1.5): 09/937961

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/AU00/00251 ✓	27 March 2000 ✓	29 March 1999 ✓

TITLE OF INVENTION: GAMING SYSTEMS AND METHODS

APPLICANT(S) FOR DO/EO/US: DONALD, Ian Forbes; SZWACH, Elik; and HORTEN, Lisa

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. [ ] The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [ ] is attached hereto (required only if not communicated by the International Bureau).
   b. [X] has been communicated by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US).
6. [ ] An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. [ ] is attached hereto.
   b. [ ] has been previously submitted under 35 U.S.C. 154(d)(4).
7. [ ] Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are attached hereto (required only if not communicated by the International Bureau).
   b. [ ] have been communicated by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [ ] have not been made and will not be made.
8. [ ] An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [ ] An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. [X] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [X] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. [X] A FIRST preliminary amendment.
14. [ ] A SECOND or SUBSEQUENT preliminary amendment.
15. [ ] A substitute specification.
16. [ ] A change of power of attorney and/or address letter.
17. [ ] A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. [ ] A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. [ ] A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. [X] Other items or information:
    Copies of prior art; return card; Certificate of Express Mailing

410 Rec'd PCT/PTO 28 SEP 2001

U.S. APPLICATION NO (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/937961	PCT/AU00/00251	M/ME/00v888US

21. The following fees are submitted:	CALCULATIONS PTO USE ONLY	
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1000.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$860.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 1000	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	34 - 20 =	14	x **$18.00**	$ 252	
Independent claims	6 - 3 =	3	x **$80.00**	$ 240	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$270.00**	$	
TOTAL OF ABOVE CALCULATIONS =				$ 1492	
☐ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2. +				$ 746	
SUBTOTAL =				$	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				$	
TOTAL NATIONAL FEE =				$	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$ 40	
TOTAL FEES ENCLOSED =				$ 786	
				Amount to be refunded:	$
				charged:	$

a. ☒ A check in the amount of $ 786.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-0620. A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO.

Alan D. Kamrath, Esq.
Rider, Bennett, Egan & Arundel, LLP
333 South Seventh Street, Suite 2000
Minneapolis, MN 55402

Alan Kamrath
SIGNATURE

Alan D. Kamrath
NAME

28,227
REGISTRATION NUMBER

410 Rec'd PCT/PTO 28 SEP 2001
09/937961

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Ian Forbes Donald, et al.
National Phase of International Appln. No.:	PCT/AU00/00251
Filed:	27 March 2000
For:	Gaming Systems and Methods
Docket No.:	16591/106 (M/ME/00V888US)

Commissioner of Patents
Washington, DC 20231

PRELIMINARY AMENDMENT

Dear Sir:

Please amend the above application as follows:

IN THE CLAIMS

Please amend claim 5 as follows:

5. A gaming system according to claim 3 wherein the telecommunications link is one of an ISDN link, an ASDL link and an IP link.

Please amend claim 7 as follows:

7. A gaming system according to claim 4 wherein:

said croupier station incorporates a croupier card reader/recorder interface,

participation in a game by the croupier is conditional upon the croupier employing an electronic croupier purse incorporated within a croupier chip-card,

said croupier chip-card also incorporates pre-recorded biometric data characteristic of the croupier as an individual human,

participation in the game by the croupier is further conditional upon computer-mediated matching of biometric data derived from the croupier with said pre-recorded biometric data, when the croupier employs said croupier chip-card to access the game, and

following access to the game, the monetary transactions are effected using said croupier purse.

Please amend claim 8 as follows:

8. A gaming system according to claim 3 wherein:

said data, audio and/or video signals are encrypted and decrypted by each station for transmission via said telecommunications link.

Please amend claim 9 as follows:

9. A gaming system according to claim 8 wherein:

said encryption is effected employing at least one encryption key that is electronically stored in each station to enable encrypting of data transmitted by said station and the decrypting of data received by said station, and

any unauthorised attempt to access said encryption keys will activate an alarm, leave an audit trail in the respective station, cause system failure or the lock-out of the station concerned.

Please amend claim 10 as follows:

10. A gaming system according to claim 6 wherein one or more of the following security violations are alarmed and/or effect system and/or station shut-down or lockout:

- any unauthorised substitution or modification of player station hardware or firmware (eg, EPROM or BIOS chips) during or prior to a game,
- any attempt to access, read or change system files in the remote player station,
- any unauthorised substitution or modification of croupier station hardware or firmware during or prior to a game,
- any unauthorised attempt to access read or change system files in the croupier station, including files containing player details and including files and processes relating to the transfer of funds from players' purses.

Please amend claim 11 as follows:

11. A gaming system according to claim 3 wherein:

each player station includes a personal EFTPOS terminal connectable to the player's bank for effecting the transfer of monetary value from the player's bank account directly into the player's purse, when the player's chip-card is activated.

Please amend claim 13 as follows:

13. A gaming system according to claim 4, wherein:

a player's identity as a person is not available to the croupier when accessing that player's station.

Please amend claim 14 as follows:

14. A gaming system according to claim 1 wherein:

said chip-card includes a fingerprint reader capable of generating read-data derived from the finger of a card user when the finger is placed appropriately on the card,

said pre-recorded data comprises fingerprint data,

access to a game by the player is contingent upon matching of said pre-recorded data with said read-data at the time of intended player access to the game, and

said matching is performed by a microprocessor incorporated within the chip-card.

Please amend claim 15 as follows:

15. A gaming system according to claim 1 wherein said player chip-card includes encrypted data effective to limit the player's access to a game according to the date or time of day of intended access.

Please amend claim 16 as follows:

16. A gaming system according to claim 1 wherein the player chip-card includes encrypted data effective to limit the maximum monetary value of a bet and/or the rate at which bets can be placed during the course of a game when employing said electronic purse.

Please amend claim 17 as follows:

17. A method for controlling operative access by a player to a player station for the purpose of gaming involving the wagering of money, comprising:

loading a chip-card into a player card reader connected to or incorporated within the player station, the chip-card having a monetary value coded therein to be adapted to serve as an electronic player purse, and the chip-card having encoded therein biometric data characterising the player as an individual human,

deriving biometric data from the player at the player station and converting the derived data into electronic form,

employing processor means within the player station or within the chip card to compare said derived biometric data with said encoded biometric data, and

providing operative access to the player station by the player upon correlation or matching of the derived and encoded biometric data.

Please amend claim 18 as follows:

18. A method according to claim 17 further including:

terminating operative access by the player to the player station upon withdrawal or removal of the player chip-card from the card reader.

Please amend claim 19 as follows:

19. A method according to claim 17 further including:

employing said processor means to read control data stored in a control register within the chip-card, and

employing said processor means to limit the functionality of the player station in accordance with said control data.

Please amend claim 20 as follows:

20. A method according to claim 19 further including:

limiting the amount of monetary value that can be transferred from the player purse to the player station for the purpose of placing a bet in accordance with said control data.

Please amend claim 21 as follows:

21. A method according to claim 20 further including:

denying player access to the player station during particular times in accordance with said control data.

Please amend claim 22 as follows:

22. A method of gaming involving monetary betting by a plurality of players operating respective computer-based player stations that are connected to one another by a telecommunications network, the method involving:

denying each player operative access to a respective player station unless a chip-card is inserted by the player into a player card reader in said station and unless biometric data pre-recorded on said card is matched with corresponding biometric data derived from the player at the station, the chip-card having a monetary value coded therein to be adapted to serve as an electronic player purse,

electronically transferring monetary value from said player purse to an electronic holding register in the player station such that the monetary value corresponds to the amount of a bet signified by player input at the station,

electronically transferring the monetary value corresponding to said bet from said holding register in a first player station to a second player station in the event that the bet at the first player is lost and the bet at the second station is won, and

electronically transferring any residual monetary value from said holding register to said purse upon termination of the game.

Please amend claim 23 as follows:

23. A method according to claim 22 further including:

terminating operative access by a player to the respective player station upon withdrawal or removal of the player chip-card from the card reader.

Please amend claim 24 as follows:

24. A method according to claim 23 further including:

employing a processor within the player card or within the player station to read control data stored in a control register within the player card inserted within the card reader, and

employing said processor means, in accordance with said control data, to limit the maximum monetary value that a player can transfer from the player card to the player station in order to place a bet.

Please amend claim 25 as follows:

25. A method according to claim 22 involving a croupier operating a computer-based croupier station that is connected to each player station by said telecommunications network, wherein transfer of monetary value to and from the holding register in each player station is effected by the croupier.

Please amend claim 26 as follows:

26. A method according to claim 25 including:

denying the croupier operative access to the croupier station unless a chip-card is inserted by the croupier into a croupier card reader in said croupier station and unless biometric data pre-recorded on said croupier card is matched with corresponding biometric data derived from the croupier at the croupier station, the chip-card having a monetary value coded therein to be adapted to serve as an electronic croupier purse,

transferring monetary values in player station holding registers corresponding to player losses to the croupier purse, and

transferring monetary values from the croupier purse to the player station holding registers corresponding to player wins,

said transfers to and from the croupier purse being under the exclusive control of the croupier.

REMARKS

For the convenience of the United States Patent and Trademark Office, enclosed are copies of the prior art cited in the parent PCT application as listed in the further enclosed FORM PTO-1449. The relevancy of the prior art is set forth in the search report for the parent PCT application. It is respectfully requested that the Examiner initial the enclosed FORM PTO-1449 and return the initialed form with the first official communication so that consideration of the prior art is of record in this application.

Favorable consideration and allowance are respectfully requested.

Respectfully submitted,

Ian Forbes Donald, et al.

Dated: September 28, 2001

By: Alan Kamrath

Alan D. Kamrath (Reg. No. 28,227)
RIDER BENNETT EGAN & ARUNDEL
333 South Seventh Street, Suite 2000
Minneapolis, MN 55402
Tel: (612) 340-8925
Fax: (612) 340-7900

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE CLAIMS

Claim 5 has been amended as follows:

5. A gaming system according to claim 3 **[or 4]** wherein the telecommunications link is **one of** an ISDN link, an ASDL link **[or]** and **an** IP link.

Claim 7 has been amended as follows:

7. A gaming system according to claim 4 **[or 6]** wherein:

said croupier station incorporates a croupier card reader/recorder interface,

participation in a game by the croupier is conditional upon the croupier employing an electronic croupier purse incorporated within a croupier chip-card,

said croupier chip-card also incorporates pre-recorded biometric data characteristic of the croupier as an individual human,

participation in the game by the croupier is further conditional upon computer-mediated matching of biometric data derived from the croupier with said pre-recorded biometric data, when the croupier employs said croupier chip-card to access the game, and

following access to the game, the monetary transactions are effected using said croupier purse.

Claim 8 has been amended as follows:

8. A gaming system according to **[any one of claims] claim** 3 **[to 7]** wherein:

said data, audio and/or video signals are encrypted and decrypted by each station for transmission via said telecommunications link.

Claim 9 has been amended as follows:

9. **[Gaming means] A gaming system** according to claim 8 wherein:

said encryption is effected employing at least one encryption key that is electronically stored in each station to enable encrypting of data transmitted by said station and the decrypting of data received by said station, and

any unauthorised attempt to access said encryption keys will activate an alarm, leave an audit trail in the respective station, cause system failure or the lock-out of the station concerned.

Claim 10 has been amended as follows:

10. A gaming system according to **[any one of claims]** **claim** 6 **[to 9 8]** wherein one or more of the following security violations are alarmed and/or effect system and/or station shut-down or lockout:

- **[Any]** **any** unauthorised substitution or modification of player station hardware or firmware (eg, EPROM or BIOS chips) during or prior to a game,
- **[Any]** **any** attempt to access, read or change system files in the remote player station,
- **[Any]** **any** unauthorised substitution or modification of croupier station hardware or firmware during or prior to a game,
- **[Any]** **any** unauthorised attempt to access read or change system files in the croupier station, including files containing player details and including files and processes relating to the transfer of funds from players' purses.

Claim 11 has been amended as follows:

11. A gaming system according to **[any one of claims]** **claim** 3 **[to 10]** wherein:

each player station includes a personal EFTPOS terminal connectable to the player's bank for effecting the transfer of monetary value from the player's bank account directly into the player's purse, when the player's chip-card is activated.

Claim 13 has been amended as follows:

13. A gaming system according to **[any one of claims]** **claim** 4 **[to 12]**, wherein:

a player's identity as a person is not available to the croupier when accessing that player's station.

Claim 14 has been amended as follows:

14. A gaming system according to **[any preceding]** claim 1 wherein:

said chip-card includes a fingerprint reader capable of generating read-data derived from the finger of a card user when the finger is placed appropriately on the card,

said pre-recorded data comprises fingerprint data,

access to a game by the player is contingent upon matching of said pre-recorded data with said read-data at the time of intended player access to the game, and

said matching is performed by a microprocessor incorporated within the chip-card.

Claim 15 has been amended as follows:

15. A gaming system according to **[any preceding]** claim **1** wherein said player chip-card includes encrypted data effective to limit the player's access to a game according to the date or time of day of intended access.

Claim 16 has been amended as follows:

16. A gaming system according to **[any preceding]** claim **1** wherein the player chip-card includes encrypted data effective to limit the maximum monetary value of a bet and/or the rate at which bets can be placed during the course of a game when employing said electronic purse.

Claim 17 has been amended as follows:

17. A method for controlling operative access by a player to a player station for the purpose of gaming involving the wagering of money, comprising **[the steps of]**:

loading a chip-card into a player card reader connected to or incorporated within the player station, the chip-card having a monetary value coded therein **[to as]** to be adapted to serve as an electronic player purse, and the chip-card having encoded therein biometric data characterising the player as an individual human,

deriving biometric data from the player at the player station and converting the derived data into electronic form,

employing processor means within the player station or within the chip card to compare said derived biometric data with said encoded biometric data, and

providing operative access to the player station by the player upon correlation or matching of the derived and encoded biometric data.

Claim 18 has been amended as follows:

18. A method according to claim 17 **further** including**:** **[the step of]**

terminating operative access by the player to the player station upon withdrawal or removal of the player chip-card from the card reader.

Claim 19 has been amended as follows:

19. A method according to claim 17 **[or 18]** **further** including **[the steps of]**:

employing said processor means to read control data stored in a control register within the chip-card, and

employing said processor means to limit the functionality of the player

station in accordance with said control data.

Claim 20 has been amended as follows:

20. A method according to claim 19 **further** including**:** **[the step of]**

limiting the amount of monetary value that can be transferred from the player purse to the player station for the purpose of placing a bet in accordance with said control data.

Claim 21 has been amended as follows:

21. A method according to claim 20 **[or 21]** **further** including**:** **[the step of]**

denying player access to the player station during particular times in accordance with said control data.

Claim 22 has been amended as follows:

22. A method of gaming involving monetary betting by a plurality of players operating respective computer-based player stations that are connected to one another by a telecommunications network, the method involving **[the steps of]**:

denying each player operative access to a respective player station unless a chip-card is inserted by the player into a player card reader in said station and unless biometric data pre-recorded on said card is matched with corresponding biometric data derived from the player at the station, the chip-card having a monetary value coded therein **[to as]** to be adapted to serve as an electronic player purse,

electronically transferring monetary value from said player purse to an electronic holding register in the player station such that the monetary value corresponds to the amount of a bet signified by player input at the station,

electronically transferring the monetary value corresponding to said bet from said holding register in a first player station to a second player station in the event that the bet at the first player is lost and the bet at the second station is won, **and**

electronically transferring any residual monetary value from said holding register to said purse upon termination of the game.

Claim 23 has been amended as follows:

23. A method according to claim 22 **further** including**:** **[the step of]**

terminating operative access by a player to the respective player station upon withdrawal or removal of the player chip-card from the card reader.

Claim 24 has been amended as follows:

24. A method according to claim 23 **[or 24]** **<u>further</u>** including **[the steps of]**:

employing a processor within the player card or within the player station to read control data stored in a control register within the player card inserted within the card reader, and

employing said processor means, in accordance with said control data, to limit the maximum monetary value that a player can transfer from the player card to the player station in order to place a bet.

Claim 25 has been amended as follows:

25. A method according to **[any one of claims]** **<u>claim</u>** 22 **[to 24]** involving a croupier operating a computer-based croupier station that is connected to each player station by said telecommunications network, wherein transfer of monetary value to and from the holding register in each player station is effected by the croupier.

Claim 26 has been amended as follows:

26. A method according to claim 25 including **[the steps of]**:

denying the croupier operative access to the croupier station unless a chip-card is inserted by the croupier into a croupier card reader in said croupier station and unless biometric data pre-recorded on said croupier card is matched with corresponding biometric data derived from the croupier at the croupier station, the chip-card having a monetary value coded therein to **[as to]** be adapted to serve as an electronic croupier purse,

transferring monetary values in player station holding registers corresponding to player losses to the croupier purse, and

transferring monetary values from the croupier purse to the player station holding registers corresponding to player wins,

said transfers to and from the croupier purse being under the exclusive control of the croupier.

TITLE: GAMING SYSTEMS AND METHODS

TECHNICAL FIELD

This invention relates to gaming systems, methods, means and apparatus involving betting or wagering where money or credit transfers take place.

In some aspects, this invention is suited to computer-mediated live gaming involving gamers who are remote from one another and/or from a gaming center (eg, a casino) but who are able to communicate in real time via telecommunication links that may include live video. The live video link in such systems may be used to show the players to one another and/or to show a croupier and gaming table to remote players.

In other aspects, the invention is suited to the regulation of gaming where the amount of an individual bet, the rate of betting, the access of individuals to games, or the like features of gaming can be controlled or regulated.

BACKGROUND TO THE INVENTION

On the one hand, there is growing concern about the social damage caused by excessive gambling and by 'problem gamblers' who do not have the financial means to support their gambling habits. On the other hand, most casinos wish to attract wealthy gamblers (herein called 'high-rollers') who play for high stakes to their tables, since they can be the most profitable of casino customers. Players of both classes may wish to be able to remain anonymous when gaming, to be able to take advantage of on-line or remote gaming via the Internet, an intranet or some private computer-mediated telecommunications network, or to be able to play between themselves without mediation by a casino croupier

From the standpoint of social policy, government authorities may wish to regulate the access of problem gamblers to casinos or gaming machines. For example, a civil court may wish to place restrictions upon a particular problem gambler, with respect to casino access, the value of bets that can be placed, the frequency of betting, the maximum amount that can be lost over a given period of time, etc. Until now, such restrictions were impractical and would have placed unworkable

obligations upon casinos. The situation is even more difficult where problem gamblers play on-line via the Internet. The present applicants are not aware of prior art that addresses these social concerns.

Of course, the situation in relation to high-rollers is quite different. Wealthy high-rollers seldom qualify as problem gamblers in the context of social policy. High-rollers generally like to participate in games involving other high-rollers but casinos cannot always arrange for such players to be present at one time. Also, many high-rollers are busy people who cannot spare the time to travel to a casino – whether in their own country or another – for the sake of one or two games. It would be desirable, therefore, to have a gaming system that allows gamblers at one or more remote locations to participate in a casino game, perhaps involving a dealer or croupier and perhaps including one or more other players at a casino table, in a realistic manner. It may also be desirable in such games to allow the players to be anonymous (with respect to one another, if not the casino), should they so desire. In any such system, however, it would be essential to ensure a high level of security in relation to the financial transactions of both the casino and the player, to safeguard the privacy of the remote player (to the degree required by the player), and to minimise the opportunity for fraud on the casino, the players or their respective banks.

In addition it would be desirable for the game to be played as realistically as possible (subject to the degree to which the identity of the players is revealed). Thus, it would be desirable for all players to see the croupier and the table or wheel (or any other gaming device), to hear any calls or comments by the croupier, to observe the cards or dice as they fall, to be able to cut a deck of cards as required, to see cards discarded or laid face-up by the croupier or other players, etc. In addition, it would be desirable for each remote player to have a supplementary visual display showing his/her hand, the bets as they are placed and as they stand, the numerical results of a throw of dice or spin of the wheel, who's turn it is to place a bet, who has passed, a textual presentation (in the player's preferred language) of any calls by the croupier, etc.

It is well known to facilitate multi-player gaming on a network such as the Internet where a computer server runs a master video game program, accepts moves from gamers and re-computes the game situation in an interactive fashion. US patent No. 5,630,757 to Gagin discloses a system of this type that employs a multi-threaded, multi-process computer operating system and a special protocol for communication via cable TV channels. Multi-player video gaming is also known where each player employs a copy of the game program on his/her PC and connects to the Internet to interact with other players who also have copies of the game. In these systems the players can remain anonymous (if desired) and live video is not an option. Such systems are not suitable for croupier-mediated interactive live gambling, nor do they allow for betting and the on-line payment of wins and losses.

It is has also been proposed to use 'electronic playing cards' in casino-mediated poker and the like games to eliminate the danger of card marking and 'cross-roading' (improper manipulation by a croupier to favour or disfavour a particular player). For example US patent No. 5,669,817 discloses the use of computer monitors for each player and for the dealer so that cards can be dealt electronically and each player's hand can be displayed to him/her alone. While 'electronic' shuffling, cutting and dealing has the advantage of avoiding croupier bias, the system of the last mentioned US patent required the croupier and players to be in the same room and all losses and wins to be settled on-site in the normal manner. No means of enabling remote play via live video, or remote settlement, was disclosed.

The participation of multiple remote players in a common board game via a network is also known. For example, US patent No. 4,372,558 discloses means whereby two remote Go players can each make physical moves (in proper sequence) on their individual boards and have the moves validated and transmitted for display to the other player. In this case, however, live interactive video and audio links are not used and no provision is made for gambling or the handling of financial transactions.

US patent No. 5,762,552 to Vuong et al discloses an interactive real-time gaming system that has provision for both audio and visual feeds and allows players at remote audio-visual terminals to place bets in more than one casino-operated game of chance at one time. However, the system is such that the remote bets must be placed at rates that are independent of rates of play of each game. This greatly limits the type of game that can be played using the system. Of most importance in the context of the present invention many – if not all – live, croupier-mediated casino games of interest to high-rollers will be excluded. In fact, the non-synchronous play feature effectively confines the system to paying multiple slot machines or other machine-generated games of chance where bets can be 'stacked' in advance of play. Though the need for financial security and authorisation is recognised by the teachings of this patent, there is no disclosure of a suitable method of implementing the necessary authorisation and security.

US patent No. 5,800,268 to Molnick discloses a method of validating the financial transactions of players who participate in a live casino game from remote locations via a communications network. Each remote player receives live television and data signals relating to a casino game at his/her remote station and uses it to convey bet information to the casino. Before the player is permitted to join a game or place a bet, the casino establishes a direct and open link to the player's bank or other financial institution that allows the casino to instantaneously (i) check that the player has enough credit to cover each bet as it is placed (ii) pay winnings directly into the player's bank account and (iii) recover losses directly from the player's bank account. The need to establish and keep open a line to each player's bank comprises considerable risk of fraud or misappropriation of that player's funds by casino employees, not to mention the loss of personal and (normally) confidential financial information belonging to the player. Even when there is no foul play on the part of the casino or its employees who are privy to the player's personal and bank account details, the personal information gained by the casino is of great value in targeting further gaming products and in selling-off such information to direct-marketing agencies.

OUTLINE OF THE INVENTION

From one aspect, the present invention is based on the use of a chip-card by a game player that incorporates an electronic purse from or to which bets, wins and losses can be transferred during the course of a game. If use of the chip-card for gaming is contingent upon biometrically matching the card to the player, the player need not be identified to a casino and there is no need for the casino to have access to the player's bank account. Moreover, the player is protected against loss or unauthorised use of the card by such biometric identification.

The use of an electronic purse in this way is well suited to remote gaming, particularly where players are provided with secure computer-based player stations capable of reading chip-cards and of being interconnected by suitable telecommunications links, preferably using data encryption to ensure security. The stations preferably have audio-visual capabilities, being adapted for text and live video display with sound and adapted to take inputs from one or more local video cameras. This allows a number of remote players to participate in a real-time, croupier-mediated game at a casino from a remote site under conditions of high security and (if desired) anonymity, yet with a high degree of realism. Given the availability of secure player stations and data encryption, the invention also permits a group of gamers to play games (eg, poker) in a pari-mutuel manner without the mediation of a live croupier. Such possibilities will suit the needs of high-rollers.

On the other hand, if gaming is contingent upon the use of such chip-cards, it will be possible for regulatory authorities to have a problem-player's electronic purse endorsed with conditions. Such conditions may affect the time when games can be accessed, the maximum amount that can be placed on any bet, the frequency of betting, or the maximum amount that can be lost or risked in a game, for example. This possibility will suit the needs of government authorities with a concerned about the social and family costs of gambling. The conditions can be recorded in the chip-card (appropriately encrypted) by the player's bank, in much the same manner as banks are required to obey court directions regarding the garnisheeing of customer's wages. The use of such cards can be required by a

casino or gaming room for access to any gaming machine, here included in the term 'player station'.

In one possible mode of croupier-mediated play, player access to a player station is conditional upon the matching of biometric parameters read from the player at the time of intended access with the same type of parameter that has been pre-recorded on the chip-card and/or in the player station. Each player station includes a chip-card interface unit or dock into which a player's chip-card must be inserted. If the read and pre-recorded biometric parameters do not match, the intended player is denied access to the station or gaming machine. After biometric identification has been effected, the player can then initiate participation in the game according to the procedures promulgated by the casino, at which point the monetary value in the electronic purse is transferred to the card reader/dock or to a secure register in the player station where it can be accessed by the croupier. Alternatively, the contents of the player purse may be transferred to an electronic casino game purse or electronic 'safe' and held in trust by the casino for the duration of the game. At the end of each betting round or game, all wins and losses can be settled by electronic transfer between the various secure registers and/or electronic purses. Such an arrangement facilitates pari-mutuel gaming with or without croupier mediation.

The croupier purse or safe can be a chip-card that is inserted by the croupier in the croupier station and that is accessed by croupier for each game by biometric identification means, as in the case of the player cards and stations. In that event, transfer of monetary value between the croupier's purse and the casino occurs in like manner to the transfer of value between the player's purse and the player's bank. However, it may be desirable to ensure that all value remaining in the casino purse at the end of a game is automatically transferred to the casino. Alternatively, the casino game purse could be a secure computer file or electronic 'safe' in the casino station, rather than a removable chip-card 'belonging to' the croupier. However, it is preferred that access to such a file by a croupier is still conditional upon biometric identification of the courier.

Conveniently, the player station may be used in association with a personal EFTPOS terminal approved by the player's bank so that monetary value can be transferred directly from the player's bank account into his/her game-card. This may be done via a bank-issued magnetic-stripe credit-card and the appropriate PINs, via a separate chip-card owned by the player using PINs or biometric identification, or via the player's gaming chip-card itself. In this way, the bank-related transactions are kept private and secure with respect to the casino staff and other players. This will not affect the casino's ability to verify (i) that the gaming chip-card has been properly validated and (ii) the amount of money in that chip-card. However, unlike the prior art system of Molnick, this can be done without disclosing any financial or personal details about the player to the casino.

Normally biometric identification will be used by each player and the croupier each time the respective chip-card is inserted in its card dock or reader, it being usual to leave the card in its dock for the duration of the game. This allows a player to permit someone else to actually play a game after it has been properly initiated. Unlike the prior art system of Molnick, this can be done without having to provide the substitute player access to the authenticated player's bank account or PINs. Alternatively, a player may elect to require biometric identification each time monetary value is transferred to or from his/her chip-card.

The particular biometric identification system or systems employed for the gaming smart-card will generally be determined by the gaming systems supplier or by the customer (usually the casino or a player syndicate). The player's bank may not require a biometric identifier, being content with a PIN-based security system. Known and commercially available biometric identification systems, based upon signature, fingerprint, voiceprint, iris or facial recognition, may be used. Most of these systems will be incorporated in chip-card readers since they are too complex or bulky for incorporation in chip-cards. For example, a fingerprint recognition system has been implemented by Netherlands Customs and a face-recognition system has developed by CSIRO and Banque-Tec of Australia for checking passports. However, a chip-card incorporating thumbprint recognition has been developed by Siemens of Germany.

A variety of measures are taken in this example to ensure system integrity and freedom from tampering, all of which can be implemented by those skilled in the art. These measures include:

- The physically integration of the input devices of a station, such as a keyboard, mouse, touch-screen, a biometric scanner and the chip-card dock, in a physically-locked casing together with the rest of the computer components. The only inputs and outputs – apart from the chip-card and its data – are, thus, encrypted electronic signals that enter and leave via multi-pin sockets.
- The elimination of removable disc-drives and memory cards other than the player's chip-card.
- Unauthorised opening of the case is alarmed and effects immediate disablement of the station and user lock-out.
- Authorised opening of the case can only be achieved upon the insertion of a service chip-card and biometric identification of the card owner.
- Any physical substitution or modification of station hardware or firmware (eg, EPROM or BIOS chips) is automatically and securely logged with data from the service card.
- Any attempt to access, read or change system or sensitive data files (eg, encryption keys) in a station by remote access via the telecommunications link is alarmed, logged and may cause disablement of the station.
- Any unauthorised substitution or modification of croupier station hardware or firmware during or prior to a game.

To implement these security provisions in respect of a player station normally requires that each player station be set up, serviced and supplied by the casino or an independent system provider. Implementation of the security provisions in respect of the croupier station will include additional procedural safeguards for effecting the transfer of cash to and from the purse or secure register of a player station.

As is normal in data communication systems involving financial transactions, the data transferred between the player's card reader and his/her station (including

video and audio signals), as well as the data transferred between the croupier station and the player station, is encrypted so that any eavesdropper will be unable to interpret that data or masquerade as a player. As already indicated, any unauthorised attempt to access encryption keys stored in either station will involve violation of station/system integrity and may cause system failure or player lock-out and, preferably, any such violation will automatically generate a recorded 'audit trail'.

The telecommunications protocol employed for communication between gaming stations can be any suitable protocol known in the art. It will conveniently be IP (Internet Protcol) if the Internet is employed. It will be generally preferable to set up a private ISDN or ASDL network for each gaming session involving high-rollers. This will generally include an ISDN or ASDL bridge (located at the casino or in the premises of the telco) and an ISDN or ASDL terminal in each player station, or gaming room. The telecommunications media employed is unimportant as far as the present invention is concerned, it being left to the telco to furnish the necessary physical connections and bandwidth. It might be expected that optical fibre and microwave/satellite trunks would be employed and that IP, ISDN and/or ASDL connections would exist at each player's premises as well as at the casino.

In the context of the present invention, the term 'casino' is used loosely to indicate any establishment that offers gaming machines or croupier-mediated games (whether the croupier is a human individual or takes the form of a computer program). The term 'chip-card' is used to indicate a card-like device that incorporates a microprocessor chip, addressable memory (whether EEPROM, EPROM, ROM or RAM) and electrical or magnetic coupling means by which the card can be connected to other electronic devices. The processor is usually adapted for cryptoprocessing (eg, the use of public/private key security, and optimised for variable-length arithmetic, modular exponentiation, asymmetric, elliptical or DES encryption under ANSI X3.92). Such cards may be issued by a certification authority that uses a special card dock which 'burns in' key data such as biometric or alphanumerical data characteristic of the owner, once the identity of the owner has been authenticated. A smart-card is a

particular form of chip-card that conforms to accepted standards, such as ISO 7810, 7812, 7816, 10536, 10373 and 14443.

An 'electronic purse' can be regarded as the configuration of a chip-card for financial transactions involving the storage and transfer of monetary value in a manner recognised by banks or other financial institutions. Such transactions are the subject of ISO TC 68, ISO SC 6 and ISO 10202. An example of an existing chip-card having an electronic-purse function is the Mondex card developed by the National Westminster Bank of the UK. The Mondex card does not require biometric identification for its use, nor does it require individual transactions to be reported back to the issuing bank. It allows the direct transfer of monetary value between Mondex cards using suitable docking stations. Since the Mondex card serves as a flexible electronic purse, it may be used in this invention, provided separate biometric identification is effected. Europay, MasterCard and Visa are reported to be developing a similar financial transaction chip-card. For convenience, the financial transaction function (and associated circuitry) of a chip-card that permits the storage and transfer of monetary value will be referred to herein as an 'electronic purse', unless otherwise indicated.

A pari-mutuel game will be taken herein to be one where the bets of losing players are transferred to the winning player(s). Pari-mutuel gaming normally does not allow players to play against the casino and is mandated in some US jurisdictions. When a pari-mutuel game is mediated by a croupier in a casino, the casino normally takes a small pre-agreed percentage of the player's stakes or transactions in each betting round, leaving the remainder of the wins and losses to be apportioned between the players.

Finally, in this specification, the term 'fingerprint' will be used to include 'thumbprint'.

DESCRIPTION OF EXAMPLES

Having generally portrayed the nature of the present invention, a particular example will now be described by way of example and illustration only. In the

following description reference will be made to the accompanying drawings, wherein:

Figure 1 is a schematic diagram of a gaming system that forms the first example of the implementation of this invention.

Figure 2 is a chart indicating the sequence of interactions between the player and casino stations during a typical gaming session employed in the system of the first example.

Figure 3 is a schematic diagram of a gaming system that forms the second example of the implementation of this invention.

Figure 4 is a schematic diagram illustrating one method of issuing a gaming card that carries a court-imposed endorsement to limit gaming by a problem gambler.

With reference to Figure 1, the gaming system 10 of the first example involves a casino 12 and two remote player locations or rooms 14a and 14b for the use of high-rollers. In this example, casino 12 includes two gaming rooms 16a and 16b and a secure computer/communications room 17. Each gaming room has a computer-based croupier station 18 fitted with a video camera 19 and a gaming table 20, all under the charge of a croupier 21. Casino communications room 17 includes a file server 22 and an ISDN video bridge 24, server 22 being connected to croupier stations 18 and to bridge 24. Of course, there may be more than two gaming rooms 14 fitted with croupier stations 18 so that multiple simultaneous games can be played and players can select which game(s) they wish to join or set-up.

Bridge 24 includes an ISDN modem and video codec. It outputs data and video signals in ISDN format to a telecommunications carrier on line 25 having ground transmit/receive dishes 26 and 28 and a satellite repeater 30. It will be appreciated that any other suitable signal protocol, such as ADSL, might be used and that the telecommunications link might just as easily be terrestrial, or a

combination of terrestrial and satellite links. The nature of the transport protocol and the link is immaterial to the present invention. For convenience of illustration, player rooms 14a and 14b are shown as each being connected to ISDN line 32 from common receiver dish 28, but it will be appreciated that the rooms may be in different countries and connected to different dishes or other telecommunication links.

Each player room 14 of this example is equipped with an ISDN interface unit 40 that which includes an ISDN modem and video codec and is connected to a computer-based player station 42, which is equipped with a video camera 44. Camera 44 may be used during a game at the option of the player(s). Player station 42 can be fitted with various player-input devices such as a touch screen, keyboard and/or mouse (which are not illustrated) but preferably has a smart-card writer/reader interface 45 built-in. If desired, rooms 14a and 14b may also be equipped with a personal EFTPOS terminal 46 that incorporates a modem, a telephone, a keypad and a swipe-slot for use with conventional magnetic stripe credit cards. EFTPOS terminal may be connected directly to player station 42 to allow monetary value to be transferred to and from a smart-card in interface 45. If desired, a video recorder and/or a printer (not shown) may be connected to player station 42 but, other than these optional connections and the essential connections to ISDN interface 40 and the power supply (not shown), the station is a sealed unit with high levels of software and mechanical security.

Player station 42 is equipped with a biometric input device (not separately illustrated) which may comprise a facial recognition program that takes its input from camera 44 or from an in-built dedicated facial scanner of a type known in th art. Alternatively or additionally, the biometric input device may be a built-in fingerprint scanner device that requires the player to press his/her finger onto a glass plate (as is also known in the art). Alternatively or additionally, the biometric input device may be a fingerprint scanner and recognition system built into the smart-card itself, as is available from Siemens of Germany.

After a player has turned on the power to player station 42, placed his/her smart-card (indicated at 47) into reader 45 and been biometrically identified, the use of

EFTPOS terminal 46 allows the player to dial his/her bank 48 via telephone lines 50 and, after use of his/her credit card and its associated PIN, to effect the loading of the smart-card using with cash (in a manner to be describe below) to establish a game purse. This will be effected without the PIN or other personal information from the player's credit card being made available to the casino or gaming system. The player's smart-card could be supplied by the casino, by the player's bank or by a third party, as preferred by the player. In either case, the supplier undertakes the initial biometric identification of the player, effects the recording of the biometric data in the card and, if desired by the player, 'loads' the smart-card purse with monetary value.

Generally, supply and installation of the player's personal EFTPOS terminal 46 will be effected by arrangement between the player and his/her bank 48. Where the player station 42 is installed in an agent's premises for use by more than one player, it will be normal for each player to simply bring his/her EFTPOS terminal 46, along with his/her smart-card 47) to the selected game (ie, room 14a or 14b).

An exemplary procedure for setting up and operating a game is illustrated by the chart of Figure 2. Once the all participating players for a particular game have been 'assembled' on-line by the casino, the players can mutually decide whether they wish to be identified or remain anonymous. If a two-way video conference system is employed, the player's monitor would normally display the other players in separate windows located around the gaming table so that their movements and expressions can be observed and their calls heard by all participants. If the players choose to be identified but not to activate the two-way video-conferencing facility, a still image selected by each player could be substituted for the live image, or no image need be used. Players can be assigned their real names or pseudonyms for the purpose of the game. These names can then appear in the appropriate places around the table (as displayed on the video monitors) and used by the croupier in oral communication with the players.

While the croupier responsible for a particular game would act exactly like a one at a conventional casino table, it is preferable that the results of a card shuffle, card deal, throw of dice or spin of the wheel be determined electronically in a truly

random manner. Thus, the cards dealt by the croupier in a card game, the fall of dice in craps, the lodgement of the ball in a roulette wheel etc, would be computer-generated and shown (as appropriate) in a window that appears in the video monitor at the appropriate time. Besides depicting face-up cards on the casino table via the video link, the casino station communicates to each player the cards dealt to him/her in a manner that is securely hidden from the croupier and other players alike. Similarly, each player station communicates to the casino station the identity of any cards discarded or turned face-up by the respective player and the results of any dice throw relegated to the player. While the casino station could determine the result of a player's dice throw using its random number generator, it is psychologically preferable that the player's station generates uses its own random number generator to determine the cast of the dice.

As in a normal casino game, however, the croupier is responsible for the management of a game, recording bets, signifying which player has the call, and resolving disputes between the players. To enhance realism when video conferencing is employed, the croupier may physically place piles of chips in each player's position or elsewhere on the gaming table to indicate the lie of bets at a given time, moving them around at the end of a round to show bets lost and won in the normal manner. The placing of bets would, of course, be communicated electronically by the players at their respective player stations to the casino/croupier. If desired, bets placed by players could be digitally incorporated into the display of the casino table as visual images of piles of chips. As it is unlikely that the monetary value of a pile of chips can be determined reliably from the monitor display at a player station, each player has the facility to interrogate the value of any bet and/or to have all bets on the table shown clearly in dollar terms on his/her monitor. Other, more general, features of a game may also be displayed upon request by a player. For example, the rules of a game, the casino 'take', whether the game is being played in pari-mutuel mode, etc.

As indicated in Figure 2, the croupier station has a 'safe' (secure computer file) in which the croupier establishes a computer account for each player, once the above mentioned preliminaries have been settled and a round of betting is about

to take place. By individual interaction with croupier, each player then effects the transfer of sufficient monetary value in his/her purse to the appropriate account in the casino safe to cover the amount that he/she is prepared to wager during the game. However, as also indicated in Figure 2, additional amounts can be transferred in this way during a game and, indeed, the player can 'top up' his/her smart-card purse using the EFTPOS terminal as the game progresses. Of course, losses and wins for each betting round are displayed on each player's station, together with the amount remaining in the player's account in the casino safe. At the end of the game, the amount remaining in the player's account is returned to the player's purse.

The second example of a gaming system, indicated at 100, is illustrated by Figure 3, where three computer-based player stations 102 are connected to one croupier computer-based station 104 in a casino 105, with or without the use of video links, cameras and live game simulation indicated in the first example. As before, each player has a chip-card 106 in which a coded biometric identifier characteristic of the player is stored, as well as an electronic purse. In contrast to the first example, however, the croupier station 104 requires the use of a croupier chip-card 108 that stores a biometric identifier of the croupier and an electronic purse. As in the case of each player, the croupier's card 108 must be in place in station 104 and the croupier must be validly identified to station 104 using the stored biometric identifier in the station and/or card before the croupier can participate in a game.

Also in contrast to the first example, each player station 102 has a secure register 110 (computer file) and, preferably, croupier station 104 also has a secure register 112. These registers serve as temporary buffers for the transfer of monetary value to and from the croupier. The croupier has access, via station 104, to all player registers 110, but no player has access to croupier's register 112 or to that of another player. Indeed, the existence of these registers need not be apparent to the players or the croupier.

During the betting round of a game, each player signifies the amount of the bet being placed. This amount is automatically transferred from his/her electronic purse in card 106 to register 110 of the respective station, the amount of the bet

being communicated to the croupier and to each other player in accordance with the rules of the game. When all bets have been placed, the monetary value in each player register 110 is transferred to croupier register 112 and, after the results of the round have been determined, monetary values representing winning bets are transferred to registers 110 of the appropriate players. This may be done automatically or at the instigation of the croupier. Either after each round or at the end of the game, all monetary value in croupier's register 112 (usually the casino's return) can be transferred to the casino or to the croupier's purse in card 108 or direct to the casino. Though not essential, the use of an electronic purse in the croupier's card may be a convenient way of establishing and quarantining a game 'bank' from larger casino funds in electronic form.

It will be appreciated that the system of the second example is well suited to pari-mutuel gaming without the participation of a croupier, particularly in games where card dealing, dice rolls, roulette wheel spins etc can be simulated by a computer and where game rules are well defined. Indeed, provided the computer system and its associated games are created, programmed, checked and marketed by reputable agents, and provided adequate security against tampering is ensured in the manner indicated, such games effectively eliminate player cheating, even where large bets are placed by players who are not identified as individuals to casinos or to one another.

In the third example, it is envisaged that access to any gaming machine or game in a casino requires the use of a chip-card having an electronic purse and the biometric matching of a player with the pre-recorded and encoded biometric parameters stored in that card. In this way, the casino can cooperate or comply with regulatory agencies concerned to limit access by problem gamblers. The manner in which chip-card can be issued to such gamblers is illustrated in Figure 3. First, there needs to be requirement that chip-cards to be used in gambling are to be specially coded and made available only through approved agents, such as banks. Second, each agent needs to be supplied with a list of court orders currently applying to problem gamblers, together with the restrictions that the court has imposed on each such person. Third the persons concerned need to properly identify themselves to the bank or other agent.

On those assumptions, and with particular reference to Figure 3, a player 200 approaches his/her bank 202 (the agent) requesting the issue of a chip-card for the purpose of gaming and requesting the transfer of funds from the player's account into the card's purse. Player 200 duly identifies himself/herself to bank 202, which then obtains a copy of the relevant court order 204 from a court 206 in paper or electronic form. The bank 202 then places a gambling chip-card 208 in an appropriate card dock or interface 210. A biometric identifier is then read from the player and encoded in a chip-card 208, together with codes representing the monetary value transferred to the purse and the restrictions applied by the court with regard to betting amounts and frequency and with regard to permitted/prohibited games. [The amount of monetary value transferable to the purse will generally be restricted as well.]

When player 200 presents the card to a casino machine or croupier (not shown), it is placed within a card reader, the player is biometrically checked and the gambling restrictions applied automatically from encoded data recorded in the card. If the restrictions permit, player 200 can transfer additional funds to card 208 using his/her PIN in a combined EFTPOS terminal and card-dock 212 connected to bank 202 via phone line(s) 214. The court restrictions encoded in the card can then be read by the bank and the appropriate limitation on funds transfer applied.

Security Considerations

(a) Fraud by a Player

The principal and most serious avenues for a player to defraud the casino or another player are (i) to place bets that he/she cannot cover, (ii) to renege on a bet or play which has been made and (iii) to employ slight of hand to substitute cards or dice etc. These actions also may be associated with the assumption of a false identity by the player.

The first two avenues for fraud are closed off according to the present invention either by the use of a game-purse, or a bet-buffer/register, accessible during a game by the croupier so that a player can be prevented from placing a bet which cannot be covered, from reneging on a bet which has been placed or from

declining to pay a lost bet to the casino or another player. The third avenue for fraud is largely avoided by the use of electronic media and 'virtual' gaming where real cards and dice are not employed. The electronic equivalent of such fraud would be the programming of the player's machine to bias or determine the result of a throw of dice or a card deal or shuffle, or to change the cards dealt in a hand. These avenues for fraud can be prevented by securing the player's station against programming access or tampering and suitably encrypting communications between players and the casino/croupier. Identification of a player as a person to the casino or to other players is not a relevant consideration in the context of this invention.

(b) Fraud by the Croupier or Casino

The outcome of games and the odds in most games of chance can be fraudulently manipulated a casino or croupier. Croupier fraud on the casino usually by 'cross-roading'. Such fraud is greatly restricted where dice throws, wheel-spins, card shuffling and the like are performed by computer. Access by the croupier to the programming of the sealed croupier station can be readily prevented with the security systems of the art.

While rigging of a game by a casino at the expense of players through manipulation of a the gaming program is certainly possible if the casino is responsible for the programming and the maintenance of the croupier stations, it can be readily checked by independent experts, if the game program is in sealed and self-contained croupier stations (not in the casino's computer system). Computer-mediated gaming also makes it easy for players to accumulate game statistics that would reveal systematic bias. Pari-mutuel gaming without the participation of the casino or the croupier, as disclosed herein, should be totally free from such cheating. Finally, as there is no need for the casino to have access to the player's bank account or banking details; or, even, to the player's identity, avenues for pressure by the casino are greatly restricted.

(c) Fraud by Third Parties

Fraud by impersonation of a player to the casino, to other players or to a bank is effectively eliminated, according to the present invention, by requiring the use of

chip-cards carrying biometric identification. A more serious threat is perhaps that where a third party can hack into the gaming system while a game is in progress, gain access to the croupier's and/or player's purse, electronically extract money therefrom and transfer it to his/her chip-card purse. Protection against this threat relies upon ensuring system integrity and security.

Ensuring System Integrity and Security

The above analysis of the risk of fraud suggests that system security is of primary concern. Hacking of the system might allow modification of random number generators, card-shuffling routines or the like, and/or access to electronic purses. Accordingly, data and video transmissions between the casino and each player are preferably encrypted using encryption keys located in both the player station and the croupier station. Many commercial encryption systems are available of sufficient power to prevent eavesdropping by third parties on transmissions between the players and casino, and, to prevent effective signal substitution. What is left, then, is the securing of the player and casino stations against unauthorised use, unauthorised access to the respective game purses and unauthorised access to the encryption keys.

To achieve the desired level of security, one or more of the following features may be incorporated in each player and the croupier station:

1. No externally accessible disc drives or connections therefor are provided so that the only ways of changing settings within the station are (i) by physical substitution of station components (eg, plug-in cards or ROM chips) and (ii) via the network using encrypted commands.
2. The station is housed within a casing that is physically locked against opening and is alarmed so that, immediately the casing is opened, key data (eg the purse software, the BIOS, all encryption keys and important hard-disc files) is deleted or the unit is otherwise crippled.
3. All key components of the player station, including the BIOS chip, are tagged with identification codes so that the system will not boot-up if any component is missing or a substitution has been detected.
4. A firmware 'dongle' is incorporated within the case and includes encryption codes essential for reading hard-disc files, for operating the computer system

and for transmitting and interpreting network messages. The dongle is connected to the system bus and battery supply in such a manner that its removal will result in the loss of its data.

5. The use of public-key infrastructure to identify and authenticate the casino and the player.
6. The use of software audit trails of all financial transactions made during a game. [Such audit trails may be mandated in some jurisdictions for all electronic financial transactions above a predetermined monetary value.]

In addition, a variety of known methods of improving the security of the chip-cards may be employed, some of which have already been mentioned. For example, key personal identifiers can be 'burnt' into the chip using fusible links so that they cannot be subsequently altered. In a similar fashion, unalterable 'firewalls' may be included in a chip-card to separate applications and/or to prevent the overwriting of data.

While it will be appreciated that the examples offer important advantages over the art, many variations and other examples are possible without departing from the scope of the invention as defined by the following claims.

****

CLAIMS

1 A gaming system wherein a player plays against a casino and/or against one or more other player participants and wherein the player is able to effect monetary transactions, including placing monetary bets, paying monetary losses and collecting monetary wins, according to the rules of a wagering game, the gaming system being characterised in that:

access to the game is conditional upon the player employing an electronic player purse incorporated within a player chip-card,

said player chip-card also incorporates pre-recorded biometric data characteristic of the player as an individual human,

access to the game is further conditional upon computer-mediated matching of biometric data derived from the player with said pre-recorded biometric data, when the player employs said player chip-card to access the game, and

following access to the game, the monetary transactions are effected using said player purse.

2 A gaming system according to claim 1 wherein:

a player card reader/recorder interface is provided for said player chip-card,

said player card interface includes means for reading said biometric data from the player at the time of intended player access to the game and for generating read biometric data therefrom, and

means are provided for matching said read biometric data derived with said pre-recorded biometric data to determine access to the game.

3 A gaming system according to claim 2 wherein:

each player plays the game using a computer-based player station incorporating said player card interface,

said player station is capable of reading the amount of monetary value within the electronic purse in a player chip-card in the card interface and is capable of transferring monetary value to or from said player purse upon input by the player to place bets or return wins, following said matching of biometric data,

said player station is computer-based and includes video, audio and/or text receive, display and transmit means, and

said player station is interconnected with other similar player stations via a telecommunications link that includes video, audio and/or data transport means, thereby permitting textual, data, voice and/or video communication between multiple players.

4 A gaming system according to claim 3 in which the game includes a croupier, the system being characterised in that:

the croupier participates in the game using a computer-based croupier station,

said croupier station is computer-based and includes video, audio and/or text receive, display and transmit means,

said croupier station is interconnected with each player station via a telecommunications link that includes video, audio and/or data transport means, thereby permitting textual, data, voice and/or video communication between the croupier and each player,

said croupier station is capable of reading the amount of monetary value transferred by a player from his/her player purse to the respective player station for the purpose of placing a bet and is capable of transferring said monetary value from the player station to the croupier station via said telecommunications link to effect acceptance of a bet, and

said croupier station is capable of transferring monetary value from the croupier station to the player station via said telecommunications link to effect payment of a win made by the respective player.

5 A gaming system according to claim 3 or 4 wherein the telecommunications link is an ISDN link, an ASDL link or and IP link.

6 A gaming system according to claim 4 wherein:

said croupier station incorporates a croupier card reader/recorder interface,

participation in a game by the croupier is conditional upon the croupier inserting a croupier chip-card in said croupier card interface,

said croupier chip-card incorporates pre-recorded croupier data characteristic of the croupier as an individual human,

participation in the game by the croupier is further conditional upon computer-mediated matching of said pre-recorded croupier data with data derived from the croupier when the croupier employs said croupier chip-card to access the game.

7 A gaming system according to claim 4 or 6 wherein:

said croupier station incorporates a croupier card reader/recorder interface,

participation in a game by the croupier is conditional upon the croupier employing an electronic croupier purse incorporated within a croupier chip-card,

said croupier chip-card also incorporates pre-recorded biometric data characteristic of the croupier as an individual human,

participation in the game by the croupier is further conditional upon computer-mediated matching of biometric data derived from the croupier with said pre-recorded biometric data, when the croupier employs said croupier chip-card to access the game, and

following access to the game, the monetary transactions are effected using said croupier purse.

8 A gaming system according to any one of claims 3 to 7 wherein:

said data, audio and/or video signals are encrypted and decrypted by each station for transmission via said telecommunications link.

9 Gaming means according to claim 8 wherein:

said encryption is effected employing at least one encryption key that is electronically stored in each station to enable encrypting of data transmitted by said station and the decrypting of data received by said station, and

any unauthorised attempt to access said encryption keys will activate an alarm, leave an audit trail in the respective station, cause system failure or the lock-out of the station concerned.

10 A gaming system according to any one of claims 6 to 9 8 wherein one or more of the following security violations are alarmed and/or effect system and/or station shut-down or lockout:

- Any unauthorised substitution or modification of player station hardware or firmware (eg, EPROM or BIOS chips) during or prior to a game,
- Any attempt to access, read or change system files in the remote player station,
- Any unauthorised substitution or modification of croupier station hardware or firmware during or prior to a game,
- Any unauthorised attempt to access read or change system files in the croupier station, including files containing player details and including files and processes relating to the transfer of funds from players' purses.

11 A gaming system according to any one of claims 3 to 10 wherein:

each player station includes a personal EFTPOS terminal connectable to the player's bank for effecting the transfer of monetary value from the player's bank account directly into the player's purse, when the player's chip-card is activated.

12 A gaming system according to claim 11 wherein:

transfer of monetary value between the player's bank and the player's card is contingent upon identification of the player using biometric means associated with the chip-card or the card reader.

13 A gaming system according to any one of claims 4 to 12, wherein:

a player's identity as a person is not available to the croupier when accessing that player's station.

14 A gaming system according to any preceding claim wherein:

said chip-card includes a fingerprint reader capable of generating read-data derived from the finger of a card user when the finger is placed appropriately on the card,

said pre-recorded data comprises fingerprint data,

access to a game by the player is contingent upon matching of said pre-recorded data with said read-data at the time of intended player access to the game, and

said matching is performed by a microprocessor incorporated within the chip-card.

15 A gaming system according to any preceding claim wherein said player chip-card includes encrypted data effective to limit the player's access to a game according to the date or time of day of intended access.

16 A gaming system according to any preceding claim wherein the player chip-card includes encrypted data effective to limit the maximum monetary value of a bet and/or the rate at which bets can be placed during the course of a game when employing said electronic purse.

17 A method for controlling operative access by a player to a player station for the purpose of gaming involving the wagering of money, comprising the steps of:

loading a chip-card into a player card reader connected to or incorporated within the player station, the chip-card having a monetary value coded therein to as to be adapted to serve as an electronic player purse, and the chip-card having encoded therein biometric data characterising the player as an individual human,

deriving biometric data from the player at the player station and converting the derived data into electronic form,

employing processor means within the player station or within the chip card to compare said derived biometric data with said encoded biometric data, and

providing operative access to the player station by the player upon correlation or matching of the derived and encoded biometric data.

18 A method according to claim 17 including the step of terminating operative access by the player to the player station upon withdrawal or removal of the player chip-card from the card reader.

19 A method according to claim 17 or 18 including the steps of:

employing said processor means to read control data stored in a control register within the chip-card, and

employing said processor means to limit the functionality of the player station in accordance with said control data.

20 A method according to claim 19 including the step of limiting the amount of monetary value that can be transferred from the player purse to the player station for the purpose of placing a bet in accordance with said control data.

21 A method according to claim 20 or 21 including the step of denying player access to the player station during particular times in accordance with said control data.

22 A method of gaming involving monetary betting by a plurality of players operating respective computer-based player stations that are connected to one another by a telecommunications network, the method involving the steps of:

denying each player operative access to a respective player station unless a chip-card is inserted by the player into a player card reader in said station and unless biometric data pre-recorded on said card is matched with corresponding biometric data derived from the player at the station, the chip-card having a monetary value coded therein to as to be adapted to serve as an electronic player purse,

electronically transferring monetary value from said player purse to an electronic holding register in the player station such that the monetary value corresponds to the amount of a bet signified by player input at the station,

electronically transferring the monetary value corresponding to said bet from said holding register in a first player station to a second player station in the event that the bet at the first player is lost and the bet at the second station is won,

electronically transferring any residual monetary value from said holding register to said purse upon termination of the game.

23 A method according to claim 22 including the step of terminating operative access by a player to the respective player station upon withdrawal or removal of the player chip-card from the card reader.

24 A method according to claim 23 or 24 including the steps of:

employing a processor within the player card or within the player station to read control data stored in a control register within the player card inserted within the card reader, and

employing said processor means, in accordance with said control data, to limit the maximum monetary value that a player can transfer from the player card to the player station in order to place a bet.

25 A method according to any one of claims 22 to 24 involving a croupier operating a computer-based croupier station that is connected to each player station by said telecommunications network, wherein transfer of monetary value to and from the holding register in each player station is effected by the croupier.

26 A method according to claim 25 including the steps of:

denying the croupier operative access to the croupier station unless a chip-card is inserted by the croupier into a croupier card reader in said croupier station and unless biometric data pre-recorded on said croupier card is matched with corresponding biometric data derived from the croupier at the croupier station, the chip-card having a monetary value coded therein to as to be adapted to serve as an electronic croupier purse,

transferring monetary values in player station holding registers corresponding to player losses to the croupier purse, and

transferring monetary values from the croupier purse to the player station holding registers corresponding to player wins,

said transfers to and from the croupier purse being under the exclusive control of the croupier.

27 A computer-based station for use by a player or a croupier in gaming where monetary bets are involved, comprising:

means adapted to connect the station to a telecommunications or computer network,

output means adapted to display and/or sound information derived from said network,

input means adapted to accept input commands for the purpose of signifying bets and plays,